



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Collaboration System (DCS)
Defense Information System Agency (DISA)

### **SECTION 1: IS A PIA REQUIRED?**

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- ☐ (1) Yes, from members of the general public.
- ☒ (2) Yes, from Federal personnel\* and/or Federal contractors.
- ☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- ☐ (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

## SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☒ New DoD Information System ☐ New Electronic Collection
- ☐ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ Yes, DITPR Enter DITPR System Identification Number
- ☐ Yes, SIPRNET Enter SIPRNET Identification Number
- ☐ No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ Yes ☒ No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent

- ☒ Yes ☐ No

If "Yes," enter Privacy Act SORN Identifier

DMDC.02 DoD

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

**Enter OMB Control Number**

**Enter Expiration Date**

☒ **No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The following authority allows Defense Collaboration System (DCS) to collect the following data:

- 5 U.S.C. 301. Departmental Regulation
- 10 U.S.C. chapter 8; 000 Directive 5105.19
- DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program
- DoD Enterprise User Data Management Plan for Persons and Personae, August 11, 2010

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose: DCS allows users to collaborate online using web conference and chat capabilities. Web conference including audio, videoconferencing, whiteboarding and security capabilities.

Category of information collected: DoD ID number as the unique identifier.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risks associated with the PII collected include revealing a user's DoD ID number. One of the ways these risks are addressed is by only using the DoD ID number for back end management purposes. Currently, a user's DoD ID number is displayed on the user's account profile. DCS will disable the display of user's DoD ID number by 1 May 2014.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

☒ **Within the DoD Component.**

Specify.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

☐ Yes

☒ No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

The DoD ID number is collected from the user upon login and is used to identify the user's profile and enable interaction with the enterprise directory.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

☐ Yes

☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The use of DoD ID number are integral to the function of the DCS system. Users cannot have a profile on the system without the use of the DoD ID number.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement

☐ Privacy Advisory

☐ Other

☒ None

Describe each applicable format.

DCS does not request users to provide PII data.

**NOTE:**

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

### **SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW**

**a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.**

**(1) What PII will be collected?** Indicate all individual PII or PII groupings that apply below.

- |                                                         |                                                 |                                                       |
|---------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------|
| <input type="checkbox"/> Name                           | <input type="checkbox"/> Other Names Used       | <input type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Truncated SSN                  | <input type="checkbox"/> Driver's License       | <input checked="" type="checkbox"/> Other ID Number   |
| <input type="checkbox"/> Citizenship                    | <input type="checkbox"/> Legal Status           | <input type="checkbox"/> Gender                       |
| <input type="checkbox"/> Race/Ethnicity                 | <input type="checkbox"/> Birth Date             | <input type="checkbox"/> Place of Birth               |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number  | <input type="checkbox"/> Personal Email Address       |
| <input type="checkbox"/> Mailing/Home Address           | <input type="checkbox"/> Religious Preference   | <input type="checkbox"/> Security Clearance           |
| <input type="checkbox"/> Mother's Maiden Name           | <input type="checkbox"/> Mother's Middle Name   | <input type="checkbox"/> Spouse Information           |
| <input type="checkbox"/> Marital Status                 | <input type="checkbox"/> Biometrics             | <input type="checkbox"/> Child Information            |
| <input type="checkbox"/> Financial Information          | <input type="checkbox"/> Medical Information    | <input type="checkbox"/> Disability Information       |
| <input type="checkbox"/> Law Enforcement Information    | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records             |
| <input type="checkbox"/> Emergency Contact              | <input type="checkbox"/> Education Information  | <input checked="" type="checkbox"/> Other             |

If "Other," specify or explain any PII grouping selected.

DoD ID number is a DMDC assigned ID number for DoD personnel.

**(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?**

The DoD ID number is collected from the user's certificate when they authenticate to the system.

**(3) How will the information be collected?** Indicate all that apply.

- |                                                                            |                                               |
|----------------------------------------------------------------------------|-----------------------------------------------|
| <input type="checkbox"/> Paper Form                                        | <input type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview                               | <input type="checkbox"/> Fax                  |
| <input type="checkbox"/> Email                                             | <input checked="" type="checkbox"/> Web Site  |
| <input checked="" type="checkbox"/> Information Sharing - System to System |                                               |
| <input type="checkbox"/> Other                                             |                                               |

If "Other," describe here.

**(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?**

The DoD ID number will be used to authorize users' access to the system, to index user profiles (profiles contain per-user configuration information), and to request additional profile information from the enterprise directory for display.

**(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?**

The PII collected will facilitate user interaction with the system and storage of user-specific configuration on the system.

**b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation?** (See Appendix for data aggregation definition.)

☐ Yes ☒ No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.



c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- ☒ Users    ☐ Developers    ☐ System Administrators    ☐ Contractors  
☐ Other

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- |                                                           |                                                   |
|-----------------------------------------------------------|---------------------------------------------------|
| <input checked="" type="checkbox"/> Security Guards       | <input checked="" type="checkbox"/> Cipher Locks  |
| <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks        |
| <input checked="" type="checkbox"/> Key Cards             | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Safes                            | <input type="checkbox"/> Other                    |

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

- |                                                                                     |                                                                                |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> User Identification                             | <input type="checkbox"/> Biometrics                                            |
| <input type="checkbox"/> Password                                                   | <input checked="" type="checkbox"/> Firewall                                   |
| <input checked="" type="checkbox"/> Intrusion Detection System (IDS)                | <input checked="" type="checkbox"/> Virtual Private Network (VPN)              |
| <input type="checkbox"/> Encryption                                                 | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> External Certificate Authority (CA) Certificate | <input checked="" type="checkbox"/> Common Access Card (CAC)                   |
| <input type="checkbox"/> Other                                                      |                                                                                |

If "Other," specify here.

**(3) Administrative Controls.** Indicate all that apply.

- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☐ Encryption of Backups Containing Sensitive Data
- ☐ Backups Secured Off-site
- ☐ Other

If "Other," specify here.

**e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?**

- ☒ Yes. Indicate the certification and accreditation status:

- |                                                                          |               |                      |
|--------------------------------------------------------------------------|---------------|----------------------|
| <input type="checkbox"/> Authorization to Operate (ATO)                  | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> Interim Authorization to Operate (IATO)         | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> Denial of Authorization to Operate (DATO)       | Date Granted: | <input type="text"/> |
| <input checked="" type="checkbox"/> Interim Authorization to Test (IATT) | Date Granted: | 18 September 2013    |

- ☐ No, this DoD information system does not require certification and accreditation.

**f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?**

There should be no impact. DoD ID number are already publicly available in user certificates, which are posted by GDS and whitepages.mil to the DoD community.

**g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?**

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Firewalls, Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) connections, access control lists, file system permissions intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the system Integrity and the data confidentiality.

**h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?**

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Firewalls, Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) connections, access control lists, file system permissions intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the system Integrity and the data confidentiality.

## **SECTION 4: REVIEW AND APPROVAL SIGNATURES**

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

### **Program Manager or Designee Signature**

NELSON.BRIDGIT.S.1241949199  
Digitally signed by NELSON.BRIDGIT.S.1241949199  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA,  
cn=NELSON.BRIDGIT.S.1241949199  
Date: 2014.03.17 08:40:51 -04'00'

Name: Bridgit S. Nelson

Title: DCS, Product Manager

Organization: Enterprise Information Services

Work Telephone Number: 301-225-5755

DSN:

Email Address: bridgit.s.nelson.civ@mail.mil

Date of Review: 17 Mar 2014

### **Other Official Signature (to be used at Component discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Other Official Signature  
(to be used at Component  
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior  
Information Assurance  
Officer Signature or  
Designee**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Privacy Officer  
Signature**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component CIO Signature  
(Reviewing Official)**

*Phurru L. Barnett* Vice CIO

Name:

*for*

David B. Bennett

Title:

Chief Information Officer

Organization:

CIO

Work Telephone Number:

301-225-8000

DSN:

Email Address:

david.b.bennett10.civ@mail.mil

Date of Review:

**Publishing:**

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: [pia@osd.mil](mailto:pia@osd.mil).

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

## APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.